

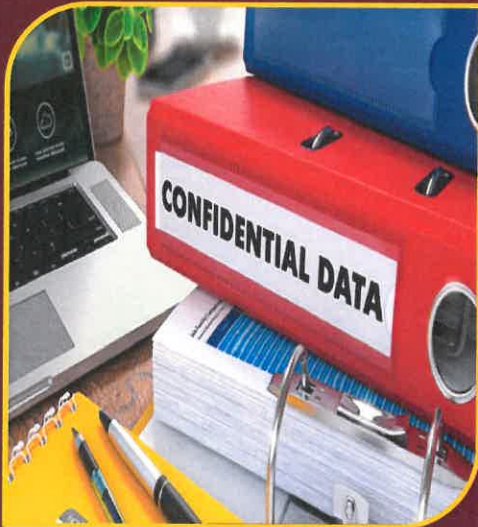
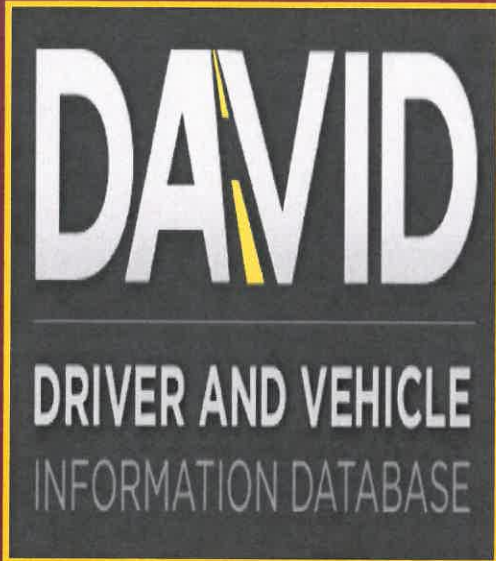


DIVISION OF INSPECTOR GENERAL

KEN BURKE, CPA

**CLERK OF THE CIRCUIT COURT AND COMPTROLLER
PINELLAS COUNTY, FLORIDA**

AUDIT OF RISK MANAGEMENT'S INTERNAL CONTROLS OVER DAVID INFORMATION

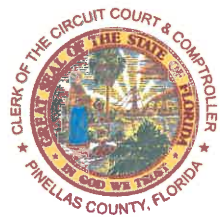


**An Accredited Office of
Inspectors General**

**Hector Collazo Jr.
Inspector General/Chief Audit Executive**

**Audit Team
Melissa Dondero, CPA, CIA, CIGA, CITP, CRMA – Assistant Inspector General
Cassy Moreau, CFE, CAMS, CIGA – Inspector General I**

**March 9, 2017
REPORT NO. 2017-03**



Ken Burke, CPA

CLERK OF THE CIRCUIT COURT AND COMPTROLLER
PINELLAS COUNTY, FLORIDA

Clerk of the County Court
Recorder of Deeds
Clerk and Accountant of the Board of County Commissioners
Custodian of County Funds
County Auditor

Division of Inspector General

510 Bay Avenue
Clearwater, FL 33756
Telephone: (727) 464-8371
Fax: (727) 464-8386
Fraud Hotline: (727) 45FRAUD (453-7283)
Clerk's website: www.mypinellasclerk.org

March 9, 2017

The Honorable Chairman and Members of the Board of County Commissioners

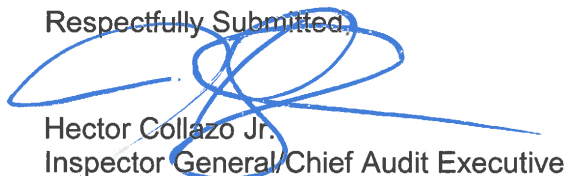
Risk Management contacted the Division of Inspector General for assistance to ensure they meet the requirements of their Memorandum of Understanding with the Department of Highway Safety and Motor Vehicles for accessing Driver and Vehicle Information Database (DAVID) data. Once Risk Management had their policies and procedures in place, they requested we conduct an audit of their internal controls over DAVID information. Our audit objectives were to:

1. Determine if adequate policies and procedures are in place to address DAVID access, distribution, use, modification, and disclosure.
2. Determine if access to the DAVID system is adequately managed.
3. Determine if appropriate logging and monitoring tools are used to manage DAVID access and use.
4. Determine if adequate physical security exists to protect confidential DAVID data from unauthorized access and use.

Risk Management has been proactive in ensuring appropriate controls are in place to protect DAVID personal data. We conclude that there is no evidence of misuse of DAVID data although Risk Management's internal controls over Motor Vehicle Record Application (MVR) access and DAVID data need improvement. Opportunities for Improvement are presented in this report.

We appreciate the cooperation shown by the Risk Management staff during the course of this review. We commend management for their responses to our recommendations.

Respectfully Submitted,



Hector Collazo Jr.
Inspector General/Chief Audit Executive

Approved:



Ken Burke, CPA*
Clerk of the Circuit Court and Comptroller
Ex Officio County Auditor
*Regulated by the State of Florida



An Accredited Office of
Inspectors General

TABLE OF CONTENTS

	Page
Introduction	4
Action Plan	6
Opportunities for Improvement	10
1. Risk Management Did Not Conduct The Required Annual DAVID Audit Prior To Signing The Annual Affirmation.	10
2. Risk Management Has Not Conducted Quarterly Quality Control Reviews Required By The MOU.	11
3. The Risk Management MVR Application, Shared Drives, And OPUS Modules Afford Access To Unauthorized Users.	13
4. The MVR SOPs Are Incomplete And Contain An Inaccurate Statement.	16
5. DAVID Inquiries Are Retained Beyond The Required Period Of Time.	18
6. The Risk Management Safety Division Does Not Have A Fully Trained Backup To Process Driver Licenses Through MVR.	19

INTRODUCTION

Synopsis

Internal controls over Driver and Vehicle Information Database (DAVID) personal data need improvement; however, we found no instances of misuse. The Risk Management Safety Division is utilizing DAVID information for appropriate business functions.

This audit was conducted at the request of Risk Management to help them comply with their Memorandum of Understanding (MOU) with the Department of Highway Safety and Motor Vehicles (DHSMV) for DAVID data. Risk Management has been proactive in ensuring appropriate controls are in place to protect DAVID personal data.

Scope and Methodology

We have conducted an audit of Risk Management's internal controls over DAVID information. The audit examined the internal controls used to protect personal data obtained through DAVID from unauthorized:

- Access
- Distribution
- Use
- Modification
- Discloser

The objectives of our audit were to:

1. Determine if adequate policies and procedures are in place to address DAVID access, distribution, use, modification, and disclosure.
2. Determine if access to the DAVID system is adequately managed.
3. Determine if appropriate logging and monitoring tools are used to manage DAVID access and use.
4. Determine if adequate physical security exists to protect confidential DAVID data from unauthorized access and use.

In order to meet the objectives of our audit, we:

- Interviewed individuals responsible for administering DAVID to obtain a clear understanding of how DAVID is accessed and used.
- Reviewed and evaluated policies and procedures addressing DAVID access, distribution, use, modification, and disclosure.

- Examined logging and monitoring tools employed for DAVID and physical security of DAVID data.
- Tested, on a sample basis, internal controls to protect personal DAVID data from unauthorized access, distribution, use, modification, and disclosure to ensure they are functioning appropriately.

Our audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* and the *Principles and Standards for Offices of Inspector General*, and accordingly, included such tests of records and other auditing procedures, as we considered necessary in the circumstances. The audit period was January 1, 2015 through October 31, 2016. However, transactions and processes reviewed were not limited by the audit period.

Overall Conclusion

There is no evidence of misuse of DAVID information since Risk Management obtained access through the Motor Vehicle Record Application (MVR); however, we found their internal controls over MVR access and DAVID data need improvement. Management has been proactive in ensuring compliance with the MOU by requesting this audit and has already implemented many of the recommendations in this report.

1. Risk Management's policies and procedures (SOPs) related to the MVR are incomplete in that they do not ensure compliance with Sections V, *Safeguarding Information*, and VI, *Compliance and Control Measures*, requirements of their MOU with the DHSMV. Furthermore, Risk Management only has one fully trained individual processing driver license inquiries, which can affect business continuity. Since discussing these issues, management has revised its SOPs and has designated an alternate person to process driver license inquiries through the MVR.
2. Our evaluation of Risk Management's administration of the MVR revealed a lack of oversight for user access to the MVR and other DAVID data repositories. Furthermore, management neither performed the required Quarterly Quality Control Reviews, nor the Annual DAVID Audits prior to submitting their Annual Affirmation to the DHSMV. Risk Management has been submitting their Annual Affirmation to DHSMV timely. Since discussing these issues, management has contacted Pinellas County Business Technology Services (BTS) about deactivating unauthorized users, and has completed both the 2016 Annual DAVID Audit and a Quarterly Quality Control Review.
3. Our testing found that the use of DAVID information was for legitimate Risk Management Safety Division business purposes.
4. Adequate physical security exists to protect confidential DAVID information from unauthorized access and use.

Action Plan

OFI NO.	OPPORTUNITIES FOR IMPROVEMENT CAPTIONS RECOMMENDATIONS	MANAGEMENT RESPONSES	IMPLEMENTATION STATUS
1	<i>Risk Management Did Not Conduct The Required Annual DAVID Audit Prior To Signing The Annual Affirmation.</i>		
	Perform the Annual DAVID Audit prior to signing the Annual Affirmation.	Concur	Planned
2	<i>Risk Management Has Not Conducted Quarterly Quality Control Reviews Required By The MOU.</i>		
	Conduct the required Quarterly Quality Control Reviews and maintain documentation for audit purposes.	Concur	In Progress
3	<i>The Risk Management MVR Application, Shared Drives, And OPUS Modules Afford Access To Unauthorized Users.</i>		
A	Provide BTS with an updated list of users who should have access to Risk Management's MVR, shared drives, and OPUS modules.	Concur	In Progress
B	Compare the Risk Management departmental users list with BTS's list to ensure accuracy.	Concur	Planned
C	Tally and verify authorized users at the departmental level, at least annually.	Concur	Planned
D	Ensure that users, whose function no longer requires access to the MVR, shared drives, and OPUS modules containing DAVID data, are deactivated within five working days as required by the MOU.	Concur	Planned

Introduction
Risk Management's Internal Controls Over DAVID Information

OFI NO.	OPPORTUNITIES FOR IMPROVEMENT CAPTIONS RECOMMENDATIONS	MANAGEMENT RESPONSES	IMPLEMENTATION STATUS
4	<i>The MVR SOPs Are Incomplete And Contain An Inaccurate Statement.</i>		
A	Review and update the MVR SOPs to meet their intended objectives.	Concur	In Progress
B	Add a troubleshooting section to the MVR SOPs to include the tips only known by the current primary user.	Concur	In Progress
C	Update the MVR SOPs to include procedures addressing the reporting requirement to the DHSMV in the event of a data security breach.	Concur	In Progress
5	<i>DAVID Inquiries Are Retained Beyond The Required Period Of Time.</i>		
A	Delete unnecessary DAVID inquiries/records from the MVR.	Concur	In Progress
B	Update the MVR SOPs to address the need for DAVID data retention in Risk Management's OPUS modules and shared drives. The SOP should also address security measures taken to ensure the safekeeping of the data.	Concur	In Progress
6	<i>The Risk Management Safety Division Does Not Have A Fully Trained Backup To Process Driver Licenses Through MVR.</i>		
	Fully train another employee to back-up the primary MVR driver license processor.	Concur	In Progress

Background

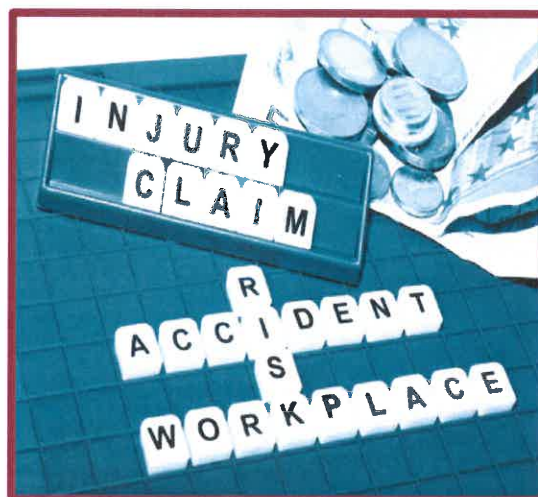
Risk Financing Administration, commonly known as Pinellas County Risk Management, administers a comprehensive risk management program that includes loss prevention and safety, claims management, insurance policy management, and contractual risk transfer. This program benefits the employees and citizens of the Pinellas County BCC, appointing authorities, and certain elected constitutional officers. As part of its responsibilities, Risk Management takes steps to develop, manage, and secure the County's most valuable assets in accordance with statutes, ordinances, and laws.



During Fiscal Year 2016, Risk Management operated on a \$10,322,620 budget, compared to an approved \$10,097,770 budget in Fiscal Year 2015. The department is comprised of a team of 16 full time employees split in three different Divisions:

- Safety
- Claims
- Insurance

The Claims Division investigates all claims, conducts pre-trial claim investigations, and attends hearings, mediations, and trials. They oversee the self-insurance program by administering claims within the self-insured retention level. The Insurance Division obtains insurance policies, when appropriate, from commercial insurance companies for the protection of various County liabilities and property. In addition, they review the majority of County contracts for insurance requirements.



The Safety Division coordinates safety policies, loss control, and safety training. It inspects facilities and jobsites to ensure National Fire Protection Association (NFPA) safety standards and Occupational Safety and Health Administration (OSHA) compliance. Its services include, new employee orientation safety training, equipment operation safety training, and cardiopulmonary resuscitation (CPR)/first aid and automated external defibrillator (AED) monitors training. They have recently embarked on a new initiative to make OSHA the standard for safety to meet the County strategic goal to make workforce safety and wellness a priority. The Safety Division also performs commercial driver license (CDL) random testing and reviews County employees' driving records. In order to fulfill the latter function, the Safety Division entered into an MOU with the DHSMV in October 2013.



The MOU gives the Safety Division access to driver and motor vehicle records in DAVID. DAVID is a multifaceted database that allows immediate retrieval of driver and motor vehicle information, including driver records, and vehicle title and registration. Unlike other governmental agencies, the Safety Division does not access DAVID directly; it does so through a driver license transcript retrieval application called MVR. This application was created and is managed by BTS. The Safety Division uses its DAVID access to review driver license transcripts of Pinellas County employees and volunteers responsible for operating County vehicles for the purpose of carrying out government functions.

The MVR system was used only for testing until February of 2016. Prior to that date, the County worked with the DHSMV, Finance, and BTS to set up the MVR application as well as an account that the DHSMV could draw from for payment of the reports. By doing this work, the County was able to save approximately \$70,000 per year, which would be the approximate cost to use a private firm to obtain MVRs.


DAVID contains confidential personal information protected by Chapter 119 of the Florida Statutes and the Driver Privacy Protection Act. Consequently, the Safety Division is tasked with ensuring the data obtained under the MOU is secure and only accessible by authorized staff. In order to comply with the requirements of the MOU, Risk Management reached out to the Division of Inspector General for assistance and requested this audit.

OPPORTUNITIES FOR IMPROVEMENT

Our audit disclosed certain policies, procedures, and practices that could be improved. Our audit was neither designed nor intended to be a detailed study of every relevant system, procedure, or transaction. Accordingly, the Opportunities for Improvement presented in this report may not be all-inclusive of areas where improvement may be needed.

1. Risk Management Did Not Conduct The Required Annual DAVID Audit Prior To Signing The Annual Affirmation.

The DAVID Annual Audit Guide provided by DHSMV instructs end users to use it to conduct their agency's Annual Audit and to prepare their Annual Affirmation.



FLORIDA
A SAFER
HIGHWAY SAFETY AND MOTOR VEHICLES

Terry L. Rhodes
Executive Director

2900 Apalachee Parkway
Tallahassee, Florida 32399-0500
www.flhsmv.gov

DAVID Audit

Below is a guide to be used to conduct your agency's annual audit and prepare the annual affirmation requested in the attached letter. The questions are taken directly from Section IV B and Section V of the MOU between your agency and the Department of Highway Safety & Motor Vehicles (DHSMV). When completed, please have the affirmation prepared pursuant to Section VI A of the MOU and mail the original signed copy to the address on the attached letter.

In addition, Section V.F. of the MOU between Risk Management and the DHSMV dated October 30, 2013 states:

"The Parties mutually agree to the following:

F. All access to the information must be monitored on an on-going basis by the Requesting Party. In addition, the Requesting Party must complete an annual audit to ensure proper and authorized use and dissemination."

Conversation with the primary MVR user revealed that prior to October 27, 2016 the department had never conducted an Annual DAVID Audit; the Annual Affirmation was being signed without it. By signing the Annual Affirmation form without performing the audit, the department has been making false statements to DHSMV since the Annual Affirmation reads:

"In accordance with Section VI., Part C, of the Memorandum of Understanding between Department of Highway Safety and Motor Vehicles and Pinellas County Board of County Commissioners, Risk Management Department (Requesting Agency) hereby Affirms that the requesting agency has evaluated and have adequate controls in place to protect the personal data from unauthorized access, distribution, use and modification or disclosure and is in full compliance as required in the contractual agreement hsmv 0134-14 (contract number)."

We recommend Management:

Perform the Annual DAVID Audit prior to signing the Annual Affirmation.

Management Response:


Management concurs and will perform the Annual DAVID Audit prior to signing the next Annual Affirmation.

2. Risk Management Has Not Conducted Quarterly Quality Control Reviews Required By The MOU.

Section IV.B.9. of the MOU between Risk Management and the DHSMV dated October 30, 2013 states:

"The Requesting Party agrees to:

- 9. ...Conduct quarterly quality control reviews to ensure all current users are appropriately authorized."*



QUARTERLY QUALITY CONTROL REVIEW REPORT

Point of Contacts (POC) can do the following to satisfy the MOU Quarterly Quality Control Review:

- Compare the DAVID Users by Agency report with the agency user list.
 - Reconcile any differences to ensure state and agency records are consistent.
- Keep a record of any new or inactivated users since the last Quarterly Quality Control Review.
 - Update any users/user information as needed, document the reason for the change in access, and the date the change is made.
- Monitor usage to ensure proper, authorized use and dissemination.
 - Randomly select a sample of users and run an audit report for a period during the quarter. Look for any misuse, including, but not limited to reason codes, running siblings, spouses, ex-spouses, celebrities, and political figures. Look at the times of day the data was accessed, repeated runs of same record, and unexplained access to the Emergency Contact Information.
 - Please note: DHSMV highly recommends the agency audit users as frequently as possible to ensure misuse is not occurring.
- Complete the below report and ensure all actions are documented.

Quarter:	Year:
Total active users in DAVID:	
Total active users in agency records:	
Users inactivated during quarter:	
Users audited during quarter:	
Total cases of misuse found:	
Total cases of misuse reported to DHSMV:	

POC Signature: _____ Date: _____

POC Name Printed: _____

Prior to our audit, the Risk Management Safety Division had never conducted a Quarterly Quality Control Review of its DAVID access. According to the primary MVR user, October 27, 2016 marked the first time Risk Management conducted the quarterly review of its DAVID access. Review of the MVR query log showed Risk Management began submitting DAVID record requests in June 2015. The records requested from June 2015 through January 2016 were for testing purposes only. On February 5, 2016, the department submitted its first official “batch” request of 200 records. Nonetheless, pursuant to the MOU requirements, a minimum of five Quarterly Quality Control Reviews should have been performed since June 2015. Overall the access to DAVID data is not adequately supervised.

Failure to conduct the Quarterly Quality Control Reviews has or could potentially have the following effects:

- Management cannot ensure DAVID queries conducted are strictly used for the purposes specifically authorized by the MOU.
- Management is non-compliant with the signed MOU.
- The County is exposed to potential liabilities due to unauthorized access to DAVID data.

We recommend management:

Conduct the required Quarterly Quality Control Reviews and maintain documentation for audit purposes.

Management Response:

Management concurs and has conducted two of the required Quarterly Quality Control Reviews since this finding. We will continue to do so each quarter. We will maintain documentation for audit purposes.

3. The Risk Management MVR Application, Shared Drives, And OPUS Modules Afford Access To Unauthorized Users.

Section IV.B.9 of the MOU between Risk Management and the DHSMV dated October 30, 2013 states:

"The Requesting Party agrees to:

Update user access permissions upon termination or reassignment of users within 5 working days and immediately update user access permissions upon discovery of negligent, improper, or unauthorized use or dissemination of information..."

Furthermore, Section V. B-G of the same MOU states:

"...The Parties mutually agree to the following:

- B. Information exchanged by electronic means will be stored in a place physically secure from access by unauthorized persons.*
- C. Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.*
- D. All personnel with access to the information exchanged under the terms of this agreement will be instructed of, and acknowledge their understanding of, the confidential nature of the information. These acknowledgements must be maintained in a current status by the Requesting Party.*
- E. All personnel with access to the information will be instructed of, and acknowledge their understanding of, the criminal sanctions specified in state law for unauthorized use of the data. These acknowledgements must be maintained in a current status by the Requesting Party.*
- F. All access to the information must be monitored on an on-going basis by the Requesting Party. In addition, the Requesting Party must complete an annual audit to ensure proper and authorized use and dissemination.*
- G. By signing the MOU, the representatives of the Providing Agency and Requesting Party, on behalf of the respective Parties attest that their respective agency procedures will ensure the confidentiality of the information exchanged will be maintained."*

Our fieldwork revealed a number of employees have unauthorized access to Risk Management's MVR, shared drives, and OPUS modules that contain DAVID data. The technical administration of user access is performed by BTS; however, the ultimate oversight responsibility for user access lies with Risk Management, the requesting party in the MOU.

As part of our audit, we asked Risk Management for a list of all of the applications used by the department as it relates to DAVID, the following list was provided:

- MVR
- PIN BCC Risk Management Reports
- PIN BCC Risk Management Update
- PIN HR-RM BI User
- Risk(H) Shared Drive
- RISKDHSMV(Z) Shared Drive

We also requested a list of the users who should have access to the respective applications. We then acquired the list of users with current access to the above applications from BTS.

Upon comparing the lists of users, we noted the following:



- Three individuals had unauthorized access to the MVR, while two other individuals who should have access did not.
- Four individuals had unauthorized access to the PIN BCC Risk Management Reports module, while three other individuals who should have access did not.
- Six individuals had unauthorized access to the PIN BCC Risk Management Update module, while three other individuals who should have access did not.
- One individual had unauthorized access to the PIN HR-RM BI User Module, while three other individuals who should have access did not.
- Nine individuals had unauthorized access to the RISK(H) drive.
- Two individuals had unauthorized access to the RISKDHSMV(Z) drive, while two other individuals who should have access did not.
- The users with unauthorized access did not sign the DAVID user acknowledgement form.
- Risk Management does not monitor user access on an on-going basis.

During our audit, Risk Management moved every folder containing DAVID data from the Risk(H) drive to the RISKDHSMV(Z) drive since every division under Risk Management, including the Safety Division, need access to the Risk(H) drive. There is a lack of oversight over user access to DAVID data; consequently, Risk Management did not comply with the MOU's requirements in Sections VI.B.9. and V.B-G.

We recommend Management:

- A. Provide BTS with an updated list of users who should have access to Risk Management's MVR, shared drives, and OPUS modules.
- B. Compare the Risk Management departmental users list with BTS's list to ensure accuracy.
- C. Tally and verify authorized users at the departmental level, at least annually.
- D. Ensure that users, whose function no longer requires access to the MVR, shared drives, and OPUS modules containing DAVID data, are deactivated within five working days as required by the MOU.

Management Response:

Management concurs and:

- A. Provided BTS with an updated list of users who should have access to Risk Management's MVR, shared drives, and OPUS modules. BTS amended accordingly.
- B. Will compare the Risk Management departmental users list with BTS's list to ensure accuracy any time there is any change in status.
- C. Will tally and verify authorized users at the departmental level, at least annually.
- D. Will ensure that users, whose function no longer requires access to the MVR, shared drives, and OPUS modules containing DAVID data, are deactivated within five working days as required by the MOU.

4. The MVR SOPs Are Incomplete And Contain An Inaccurate Statement.

The objectives of Risk Management's "Procedure to Run County Driver's through the State Database using MVR" are to:

- *"Ensure proper County DL checks are confidential"*
- *Ensure that documents are created following proper procedures*
- *Provide documentation of procedures for State Agreement"*

Furthermore, it is considered best practice for SOPs to be complete enough to address most eventualities during the course of business and so any staff can follow them.



The MVR SOPs are a compilation of step by step procedures to prep DAVID requests, to submit the requests to DHSMV, and to retrieve/view their response through MVR, among other things.

In order to test the effectiveness of the MVR SOPs, the auditor performed a walkthrough with the primary user. The auditor read the instructions to the primary user while she was executing them. Overall, the exercise revealed:

1. The MVR SOPs state:

"Once everything is in place the Primary User will contact the Division of the Inspector General [IG]. They will set up a yearly audit to ensure compliance."

According to Section VI., Part C of the MOU between Risk Management and DHSMV, Risk Management is to submit an Annual Affirmation to DHSMV affirming they have evaluated and have adequate controls in place to protect the DAVID data from unauthorized access, distribution, use, modification, and disclosure and are in full compliance as required by the MOU.

In order to affirm their compliance annually, Risk Management must perform an Annual Audit of their internal controls over DAVID themselves. The audit task could only be transferred to the Division of Inspector General (IG) upon written approval from the DHSMV; however, on October 27, 2016, DHSMV denied the transfer of the audit function to the IG.

2. Sections 5.3, 5.5.2, and 5.8 of the SOPs are incomplete; as the auditor was dictating the steps from these sections, the primary user noted some steps missing:
- a) 5.3 (*Gather information for the period*)
 - b) 5.5.2 (*Create the New Hire listing and get it ready for MVR*)
 - c) 5.8 (*Retrieving information from the response folder*)

3. Some crucial troubleshooting tips are not included in the SOPs. As of now, only the primary user knows them since she has been the main employee driver license processor.
4. The MVR SOPs do not address the reporting requirement to DHSMV should there be a data security breach. Section VI.B. of the MOU states:

"The Requesting Party must immediately notify the Providing Agency and the affected individual following the determination that personal information has been compromised by any unauthorized access, distribution, use, modification, or disclosure. The statement to the Providing Agency must provide the date and the number of records affected by any unauthorized access, distribution, use modification, or disclosure of personal information. Further, as provided in section 817.5681, Florida Statutes, the document must provide a statement advising if individuals whose personal information has been comprised have been notified and, if not, when they will be notified. The statement must include the corrective actions and the date these actions are completed by the Requesting Party."

It would be considered best practice for Risk Management to establish and incorporate procedures addressing the reporting requirement in the MVR SOPs in the event of a security breach.

Inadequate standard policies and procedures can impede Risk Management Safety Division's daily operation, result in noncompliance with the MOU, and could cause the County to incur liabilities.

We recommend Management:

- A. Review and update the MVR SOPs to meet their intended objectives.
- B. Add a troubleshooting section to the MVR SOPs to include the tips only known by the current primary user.
- C. Update the MVR SOPs to include procedures addressing the reporting requirement to the DHSMV in the event of a data security breach.

Management Response:

Management concurs and:

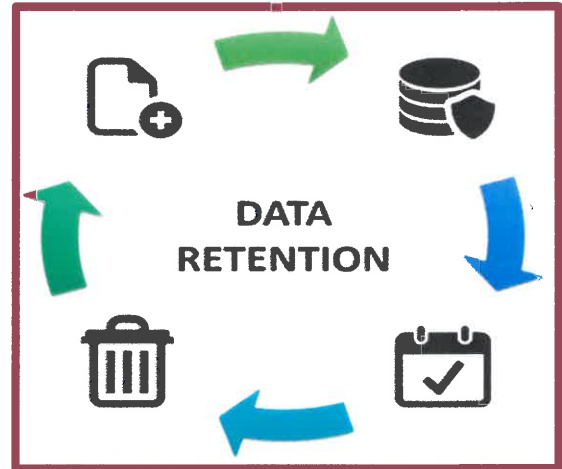
- A. Reviewed and updated the MVR SOPs to meet their intended objectives.
- B. Added a troubleshooting section to the MVR SOPs to include the tips only known by the current primary user.

- C. Updated the MVR SOPs to include procedures addressing the reporting requirement to the DHSMV in the event of a data security breach.

5. DAVID Inquiries Are Retained Beyond The Required Period Of Time.

Section IV.B.1. of the MOU between Risk Management and the DHSMV dated October 30, 2013 states:

"The Requesting Party agrees to: 1. For the Requesting Party, driver license and/or motor vehicle, information may only be used for the express purposes described herein. Information obtained from the Providing Agency by the Requesting Party shall not be retained by the Requesting Party, unless obtained for a law enforcement purpose or resold to any Third Party."



During our fieldwork, we noted the inquiries made by Risk Management since it gained access to DAVID are stored in the MVR. The auditor inquired how long the information is needed for; the primary user indicated the inquiries are no longer needed after two months. In the presence of Risk Management's Database Administrator (DBA) for MVR, the auditor suggested the inquiries/records be deleted once they are no longer needed. The DBA explained he could have it setup so the records would be automatically deleted after a set period of time.

In addition, some of the DAVID data obtained through the MVR inquiries is captured in Risk Management's OPUS modules and also saved in Risk Management's shared drives. The information is used for the purpose expressed in the MOU and maintained for business continuity. It would be considered best practice for the SOPs to address the MOU's data retention requirement and Risk Management's need to retain some of the DAVID data.

We recommend Management:

- A. Delete unnecessary DAVID inquiries/records from the MVR.
- B. Update the MVR SOPs to address the need for DAVID data retention in Risk Management's OPUS modules and shared drives. The SOP should also address security measures taken to ensure the safekeeping of the data.

Management Response:

Management concurs and:

- A. Deleted unnecessary DAVID inquiries/records from the MVR. Risk added a requirement in SOPs that every thirty days a request is sent to BTS to clear unnecessary inquiries/records.
- B. Updated the MVR SOPs to address the need for DAVID data retention in Risk Management's OPUS modules and shared drives. The SOP now addresses security measures taken to ensure the safekeeping of the data. Measures include data being stored on the "Z" drive with BTS controlling access to authorized users only.

6. The Risk Management Safety Division Does Not Have A Fully Trained Backup To Process Driver Licenses Through MVR.

From a going concern stand point, it is considered best practice to have at least two employees cross-trained in any given function to avoid business interruption should the main employee not be available.

During a walkthrough of the MVR SOPs, the auditor noted some important troubleshooting tips are not included in the SOP. As of now, only the primary user knows them since she has been handling the processing of driver licenses for employees. Should the primary user not be available, the incompleteness of the SOPs could impede driver license processing through MVR.

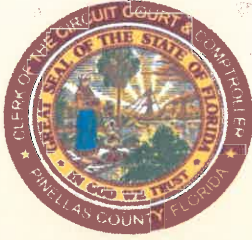


We recommend Management:

Fully train another employee to back-up the primary MVR driver license processor.

Management Response:

Management concurs and has fully trained another employee to back-up the primary MVR driver license processor.



DIVISION OF INSPECTOR GENERAL

KEN BURKE, CPA
CLERK OF THE CIRCUIT COURT
& COMPTROLLER
PINELLAS COUNTY, FLORIDA

SERVICES PROVIDED

AUDIT SERVICES

INVESTIGATIONS

GUARDIANSHIP SERVICES

CONSULTING

TRAINING

COUNTY FRAUD HOTLINE

GUARDIANSHIP FRAUD HOTLINE

PCSO PREA HOTLINE



An Accredited Office of
Inspectors General

Call: (727) 464-8371

Fax: (727) 464-8386

Fraud: (727) 45FRAUD

(727) 453-7283



Internet: www.mypinellasclerk.org

 www.twitter.com/pinellasig

 www.facebook.com/igpinellas



Write:

Division of Inspector General

510 Bay Avenue

Clearwater, FL 33756